**Identificación de equipos Windows en red**

**NetBIOS →** Es un protocolo de la capa OSI de sesión que permite que los equipos puedan compartir recursos en red.

Todos los sistemas Windows incluyen NetBIOS, ya que siempre lo han usado para nombrar equipos y grupos de trabajo.

A nivel histórico, en 1984 IBM diseñó una API para conectar en red sus computadoras,

**SMB/CIFS**

SMB es un protocolo de red de la capa de aplicación en TCP/IP que permite compartir archivos e impresoras en redes Windows. En el modelo OSI, suele usarse en la capa de aplicación o presentación, dependiendo de protocolos inferiores para el transporte.

SMB fue desarrollado por IBM, pero Microsoft lo modificó ampliamente. En 1998, Microsoft lo renombró como CIFS, añadiendo soporte para enlaces simbólicos, hard links y archivos más grandes. Además, la versión de Microsoft incluye características no presentes en el SMB original.

**SAMBA**

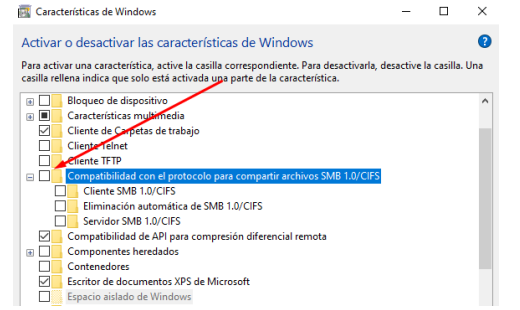
Samba es una implementación libre del protocolo de archivos compartidos de Windows para sistemas UNIX. Permite que computadoras con GNU/Linux, Mac OS X o Unix funcionen como servidores o clientes en redes de Windows.

**Vulnerabilidades asociadas con SMB**

La NSA lanzó exploits contra **SMBv1**, un protocolo antiguo y vulnerable, permitiendo ejecución de comandos con privilegios administrativos. Estas fallas fueron aprovechadas por amenazas como **EternalBlue** y **EternalRomance**, facilitando la propagación de malware como **Emotet, TrickBot, WannaCry y NotPetya**.

Por ello, Microsoft recomienda deshabilitar SMBv1 para reducir riesgos de ataques y malware.

**Deshabilitar SMBv1**



**Instalación de SAMBA**

* **smbd:** proporciona el servicio SMB/CIFS.
* **nmbd:** El demonio nmbd proporciona el servicio de nombres NetBIOS, escucha solicitudes del servidor de nombres y permite que otras computadoras en la red encuentren el servidor Samba.

Una vez iniciado, smbd escuchará en los puertos TCP 139 y 445; y nmbd escuchará en los puertos UDP 137 y 138.

* **TCP 139:** utilizado para compartir archivos e impresoras y otras operaciones.
* **TCP 445**: el puerto CIFS sin NetBIOS.
* **UDP 137**: utilizado para la exploración de redes NetBIOS.
* **UDP 138**: utilizado para el servicio de nombres NetBIOS.

